

ORIGINAL

AO 91 (Rev. 11/82)

## CRIMINAL COMPLAINT

|   |  |   |                                     |
|---|--|---|-------------------------------------|
| UNITED STATES DISTRICT COURT  |  | CENTRAL DISTRICT OF CALIFORNIA  |                                     |
| UNITED STATES OF AMERICA<br>v.<br>ANTHONY SCOTT LLOYD   |  | DOCKET NO.  |                                     |
|   |  | MAGISTRATE'S CASE NO.<br><b>17MJ 02814</b>  |                                     |
| Complaint for violation of Title 18, United States Code, Section 115(a)(1)(B)   |  |   |                                     |
| NAME OF MAGISTRATE JUDGE<br>THE HONORABLE SUZANNE H. SEGAL  |  | UNITED STATES<br>MAGISTRATE JUDGE   | LOCATION<br>Los Angeles, California |
| DATE OF OFFENSE<br>October 22, 2017   | PLACE OF OFFENSE<br>Los Angeles County | ADDRESS OF ACCUSED (IF KNOWN)   |                                     |
| COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:<br><br>[18 U.S.C. § 115(a)(1)(B)]<br><br>On or about October 22, 2017, in Los Angeles County, within the Central District of California, defendant ANTHONY SCOTT LLOYD ("LLOYD") threatened to murder a United States official, namely United States Congresswoman Maxine Waters, with the intent to impede, intimidate, or interfere with Congresswoman Waters while engaged in the performance of official duties, or with intent to retaliate against Congresswoman Waters on account of the performance of her official duties, in violation of Title 18, United States Code, Section 115(a)(1)(B), influencing, impeding, or retaliating against a Federal official. |  | <div style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;">FILED<br/>CLERK, U.S. DISTRICT COURT</p> <p style="text-align: center;">NOV - 8 2017</p> <p style="text-align: center;">CENTRAL DISTRICT OF CALIFORNIA<br/>BY <i>MA</i> DEPUTY</p> </div> |                                     |
|   |  |   |                                     |
| BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:<br><br>(See attached affidavit which is incorporated as part of this Complaint)  |  |   |                                     |
| MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A  |  |   |                                     |
| Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.   |  | SIGNATURE OF COMPLAINANT<br><i>[Signature]</i>  |                                     |
|   |  | OFFICIAL TITLE<br>Special Agent – FBI   |                                     |
| Sworn to before me and subscribed in my presence,   |  |   |                                     |
| SIGNATURE OF MAGISTRATE JUDGE <sup>(1)</sup><br><i>[Signature]</i>  |  |   | DATE<br>November 8, 2017            |

<sup>(1)</sup> See Federal Rules of Criminal Procedure 3 and 54

**AFFIDAVIT**

I, Christopher L. Kontsis, being duly sworn, declare and state as follows:

**I. INTRODUCTION**

1. I am a Special Agent ("SA") with the United States Federal Bureau of Investigation ("FBI"), and have been so employed since April 1996. I am currently assigned to the Violent Crimes-Major Offenders/Gangs Squad 1 of the Long Beach Resident Agency of the Los Angeles, California Field Office.

2. During the course of 21 years in federal law enforcement, I have conducted numerous investigations pertaining to violations of federal and state laws within the southern Los Angeles County area, including threats to assault, kidnap or murder. I have participated in the execution of numerous federal and state search warrants and arrest warrants. As part of my basic training with the FBI, I received training in tactics, conducting interviews, and conducting federal criminal investigations. I am familiar with the methods and characteristics of those who threaten public officials and the use of digital devices in connection with threats offenses.

**II. PURPOSE OF AFFIDAVIT**

3. This affidavit is submitted in support of the following:

a. A complaint and arrest warrant charging ANTHONY SCOTT LLOYD with making threats against a United States official, in violation of 18 U.S.C. § 115(a)(1)(B).

b. An application for a warrant to search the cellular telephone with the number (310) 415-8873 ("LLOYD'S PHONE"), as further described in Attachment A for evidence, fruits, or instrumentalities of the violation of 18 U.S.C. 18 U.S.C. § 115(a)(1)(B) (Criminal Threat Against United States Official) (the "SUBJECT OFFENSE"). Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my knowledge, training, and experience, and information obtained from various law enforcement personnel and witnesses, the collective experiences related to me by other FBI SAs and my review of reports written by U.S. Capitol Police SA Deborah Lippay and FBI Task Force Officer ("TFO") Tucker Kleitsch. I have also reviewed supporting documents in this matter, including the audio and video recordings relating to the interview described herein. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

### **III. SUMMARY OF PROBABLE CAUSE**

5. On October 22, 2017, ANTHONY SCOTT LLOYD called U.S. Congresswoman Maxine Waters on her Washington, D.C. office line from his cell phone and left a threatening voicemail, specifically threatening to kill her if she continues making

**Instrumentality Protocol**

comments regarding the President. LLOYD has admitted to using LLOYD'S PHONE to leave the voicemail, to look up Congresswoman Waters' contact information, and for other activities related to his threat against Congresswoman Waters.

#### IV. STATEMENT OF PROBABLE CAUSE

6. On October 24, 2017, I was contacted by the FBI Washington Field Office ("WFO") and asked to interview ANTHONY SCOTT LLOYD regarding an October 22, 2017 threatening voicemail sent to U.S. Congresswoman Maxine Waters' Washington, D.C. Office (the "Voicemail"). I listened to a copy of the Voicemail that was provided by WFO. The Voicemail was left by a male and stated: "This message is directed to Maxine Waters herself. If you continue to threaten the President, which you've done this morning with your comments about you're going to, what you said at your little faggot conference, if you continue to make threats towards the President, you're going to wind up dead, Maxine, 'cause we'll kill you. You can call the FBI, you can call the NSA, you can call whoever the fuck you want and report this and try to get a surge or some kind of fucking phone number. Bitch, if you do it again, you're dead. You're a fucking dead ass nigger." Based upon my training and experience, as well as the tone of the message and the verbiage used, I considered the Voicemail to be a valid threat against

Congresswoman Waters intended to intimidate or retaliate against the Congresswoman.

7. Based on my review of reports prepared by FBI TFO Tucker Kleitsch and U.S. Capitol Police SA Deborah Lippay, I learned the following:

a. On October 23, 2017, Zachary Cooper, Staff Assistant, Office of Congresswoman Maxine Waters, 2221 Rayburn House Office Building, Washington D.C., telephonically contacted the U.S. Capitol Police ("USCP"), Threat Assessment Section ("TAS") and spoke with SA Lippay. Cooper reported a threatening voicemail message (the Voicemail) that was received on October 22, 2017 at approximately 12:51 p.m. EST. The call was received on the Congresswoman Waters main office telephone number (202) 225-2201. Cooper provided SA Lippay access to Congresswoman Waters' voicemail system.

b. SA Lippay accessed the voicemail system and listened to the Voicemail. Caller ID indicated the call was received on Sunday, October 22, 2017 at 1251 hours. SA Lippay made a digital copy of the Voicemail.

c. SA Lippay called the Verizon/LEO access number and prepared a Verizon Emergency Situation Disclosure Request By Law Enforcement form for incoming records for Waters' office line, telephone number (202) 225-2201, time frame 12:21 p.m. to 1:21 p.m. EST, for October 22, 2017.

d. Verizon results indicated there was an incoming call from telephone number (310) 415-8873 (the phone number of

LLOYD'S PHONE) to telephone number (202) 225-2201 on October 22, 2017 at 16:50:23 GMT time with a call duration of one minute and 33 seconds.

e. SA Lippay dialed (310) 415-8873 and was greeted by a voicemail message in which a male voice identified himself as "ANTHONY LLOYD." SA Lippay conducted a law enforcement database search for telephone number (310) 415-8873 that produced one record, and that record was for ANTHONY LLOYD, date of birth December 9, 1972, California Driver's License Number D7987200. SA Lippay conducted a database check for D7987200, which produced LLOYD's California DMV information, including a residential address in San Pedro, California.

8. On October 30, 2017, I telephonically interviewed Zachary Cooper and learned the following information.

a. Cooper stated that one of his job responsibilities is to screen telephone calls and routinely check the voicemail system for messages left on Congresswoman Waters' main telephone number for her legislative office in Washington D.C. Cooper advised that whenever Congresswoman Waters makes a statement about the President, the office receives an "up-tick" in telephone calls and voicemail messages.

b. Cooper stated that Congresswoman Waters made some statements about the President over the weekend of October 21, 2017. On October 22, 2017, at approximately 6:57 p.m., Cooper accessed Congresswoman Waters' telephone system from his residence via his work cell phone. Cooper listened to a voicemail that was left by a male in which the male threatened

to kill Congresswoman Waters (the Voicemail). Upon hearing the Voicemail, Cooper became "very concerned for the Congresswoman's safety." Cooper stated the Congresswoman receives numerous "hateful" and "harassing" voicemail messages, but rarely does she receive a threatening message in which the caller used the word "kill."

c. At approximately 7:24 p.m. that same evening, Cooper called Congresswoman Waters on her cell phone and told her he listened to a threatening voicemail (the Voicemail) and was concerned for her safety. Congresswoman Waters asked Cooper what was said in the voicemail and Cooper told her. Congresswoman Waters told Cooper to contact the USCP.

d. On October 23, 2017, Cooper contacted the USCP and spoke with SA Lippay and reported the Voicemail.

9. On October 27, FBI SA Mark Matthews and I interviewed ANTHONY SCOTT LLOYD at 1743 Miracosta Street, San Pedro, California 90732. The interview was covertly recorded with audio and video. The following information, among other information, was obtained during the interview:

a. LLOYD was living with his grandmother, Anna Marie Zuanich, who was present at times during the interview.

b. LLOYD believed agents were there regarding videos that were being posted by an individual named David Smith on YouTube and one video in particular where Smith threatened LLOYD. I advised LLOYD that we were not there because of the videos and asked him to explain. LLOYD advised that Smith was posting videos on YouTube subsequent to the Las Vegas shooting

in which Smith was encouraging people to shoot cops. LLOYD left comments on Smith's videos indicating he did not agree with Smith. The two began to exchange comments with one another via YouTube. LLOYD stated that Smith posted a video where he was taunting LLOYD while racking a 12 gauge shotgun. After watching the video, LLOYD stated: "So I was like fine, I'm gonna go after this man and I'm gonna fucking kill him." LLOYD then advised that "on his way out of town to do that" he stopped at Los Angeles Police Department Harbor Division and showed them the video and filed a report. LLOYD stated that he was "heading out of town to go deal with him." LLOYD was upset that Smith posted a video directed at him while holding a shotgun. SA Matthews asked LLOYD if he was really going to hurt Smith. LLOYD replied, "Yeah." SA Matthews asked LLOYD to elaborate on what exactly he was going to do. LLOYD stated: "I was going to show up to his pad and there was going to be a confrontation. And I knew if I showed up to his pad and there was a confrontation, he would probably get violent, and if he got violent, I was going to kill him." LLOYD further advised that he was planning on taking a gun. LLOYD advised that he did not own any guns, but that he was going to go get one. Later in the interview, LLOYD again stated that he did not own any weapons, that the only person he knew who owned weapons lives in Alaska, and that he had no intention of actually taking a gun to Smith's residence.

c. LLOYD said he felt he was being threatened by Smith in the videos and believed that Smith could show up to his house and harm him and his grandmother.



d. LLOYD said that after Smith made the comments on YouTube, LLOYD researched Smith and found he owned DKS Media Solutions. LLOYD researched DKS Media Solutions and believed Smith to be a photographer. Later in the interview, LLOYD stated that Smith lived in Los Angeles and that he knew Smith's address, which LLOYD got from DKS's website. LLOYD stated the he told the officers at LAPD Harbor Division that if Smith showed up on his doorstep, "I'm not calling you. I'm telling you. I'll wait for his pulse to stop and then I'll call you because I want to ensure that he's dead. And I told them that. I'll do it first, wait for him to die, then I'll call ya. And you can bring the morgue out."

e. LLOYD told us that he contacted "Agent Dickson" regarding the videos being posted by Smith. LLOYD said he talked on the phone with Agent Dickson and exchanged e-mails with Agent Dickson. LLOYD said he thought Agent Dickson was an FBI Agent, but when he showed me the signature block of an e-mail he received from Agent Dickson, I saw that Dickson worked for the Los Angeles Police Department, Counter Terrorism & Special Operations Bureau, Major Crimes Division - FBI Task Force. LLOYD stated that Agent Dickson told him he was trying to get a warrant for Smith.

f. LLOYD stated the he contacted YouTube and filed a formal complaint seven times for seven videos that were posted by Smith.

g. LLOYD provided his cellular telephone number as (310) 415-8873 (LLOYD'S PHONE), the number that left the Voicemail.

h. I advised LLOYD that the FBI was at his house because of the voicemail message he left for Congresswoman Maxine Waters on Sunday, October 22, 2017, on her Washington D.C. office telephone. I played a copy of the Voicemail for LLOYD. I asked LLOYD if he recalled leaving the message. LLOYD replied, "Yeah, but there's nothing to it." LLOYD was upset that Congresswoman Waters was making "veiled" comments about doing something to the President.

i. LLOYD recalled that on Sunday morning October 22, 2017, he was probably parked in his car in San Pedro waiting for his friend to walk her dog. He was listening to talk radio and it was "spur of the moment" that he decided to call Congresswoman Waters. LLOYD said that he was going to "make a statement" because "his voice matters." LLOYD stated that after he left the Voicemail he thought "you probably could have done that one better." LLOYD stated that his told his friend "Tara" about the Voicemail and she told him he was an "idiot" and to not be surprised if he got a knock on the door. LLOYD told Tara that he was not harmful to anybody.

j. Regarding the Voicemail, LLOYD stated that the point he was trying to drive home was, "bitch if you make a move on my President . . . your ass is in trouble. You better not make a move on the President, you better not encourage people to make a move on the President, because if you do, it's all over,

what are you crazy? If you're out there making statements like that and somebody does something, It's on you."

k. LLOYD stated that he has no intentions of harming Congresswoman Waters. He also stated that the last time he visited Washington, D.C. was in 1982. LLOYD stated that he does not know where Congresswoman Waters's Los Angeles Office is located.

l. LLOYD said he follows the news "religiously" and was upset that Waters is constantly making comments about the President. LLOYD looked at me and stated: "I don't know if you follow the news or not. How much you follow the news. You're not the type of guy that gets riled up probably."

m. When questioned if he was a Pro-Trump supporter, LLOYD advised that he was a "pro-President supporter."

n. LLOYD stated: "It just infuriates the hell out of me to hear people talking about going after a president, we're gonna, you know, send our people to handle a president, she has this Antifa group."

o. LLOYD advised that he had used his cell phone to look up the telephone number for Maxine Waters. LLOYD said he was so "worked up" by what Maxine Waters said and what she was alluding to.

p. I asked LLOYD that if he was Maxine Waters and received that voicemail, would he think someone was trying to kill him. LLOYD replied: "I understand. I understand. Her yes, anybody but me, yeah." LLOYD indicated that he personally would not be concerned by receiving that voicemail. I asked

LLOYD if he thought a common person would be fearful if they received that voicemail. LLOYD replied: "Probably."

q. When questioned about his mental health or if he was on medication, LLOYD stated: "I'm not crazy, I'm not under any medication, I'm not a pre-meditator, I'm not a planner, I'm not a terrorist guy, I'm very patriotic and I love my country."

10. On October 24, 2017, I conducted a database search of the Automated Firearms System, which revealed that ANTHONY SCOTT LLOYD did not have any firearms registered to him.

11. On October 25, 2017, I learned from Verizon that the subscriber for telephone number (310) 415-8873 was Anna Zuanich, the name of LLOYD'S grandmother, and listing the residential address where I visited LLOYD in San Pedro, California.

12. For all the reasons described above, there is probable cause to believe LLOYD has committed a violation of Title 18 U.S.C. Section 115(a)(1)(B). In addition, there is probable cause to believe evidence of the SUBJECT OFFENSE will be found on LLOYD'S PHONE.

#### **V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES**

13. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including mobile telephones, and smart phones; and memory cards. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of

digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to

search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.<sup>1</sup> Electronic files saved to a hard drive or storage on a phone can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an

---

<sup>1</sup> These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, an operating system may also keep a record of deleted data in a swap or recovery file.

Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache.

The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive and storage on a phone requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital

devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. File systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.



f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal

data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

14. I know from my training and experience and my review of publicly available materials that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will

unlock the device. In my training and experience, users of devices with a fingerprint sensor feature often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security.

15. In some circumstances, fingerprint sensors will not work, and a passcode must be entered to unlock the device. For example, with Apple's Touch ID feature, these circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked; and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made. Other brands have similar restrictions. I do not know the passcodes of LLOYD'S PHONE.

16. For these reasons, while executing the warrant, agents will likely need to use LLOYD'S fingerprints or thumbprints to attempt to gain access to LLOYD'S PHONE if it is a fingerprint sensor-enabled device while executing the search warrant. The

warrant seeks the authority to compel the use of LLOYD'S fingerprint and/or thumbprint during the execution of the search of LLOYD'S PHONE. The government may not be able to obtain the contents of the devices if those fingerprints are not used to access the devices by depressing them against the fingerprint sensor at the time of the search. Although I do not know which of the fingers are authorized to access on any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

17. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.


//

//

//

VI. CONCLUSION

13. For all the reasons described above, there is probable cause to believe that LLOYD committed the SUBJECT OFFENSE and that evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSE will be found in LLOYD'S PHONE.



Christopher L. Kontsis Special  
Agent

Federal Bureau of Investigation

Subscribed to and sworn before me  
this 8 day of November 2017.



HONORABLE SUZANNE H. SEGAL  
UNITED STATES MAGISTRATE JUDGE

Instrumentality Protocol